CLAIMS:

1. A method to detect unauthorized reconnaissance or scanning of a computer network comprising the acts of:

(a) monitoring communications within the network;

(b) detecting predefined sequence of packets flowing within said communications; and

(c) issuing an alert indicating unauthorized scanning if the predefined sequence of packets is detected.

2. The method of claim 1 wherein the monitoring is done within a selected network device.

3. The method of claim 1 or claim 2 wherein the detecting act further includes the acts of providing a histogram in which states of the predefined sequence of packets are maintained; and

dynamically updating said histogram as selected ones of the predefined sequence of packet is detected.

4. The method of claim 3 wherein the histogram includes a table partitioned into a first field in which source addresses of network devices are kept; and

a second field, concatenated to the first field, in which a code representing states in which packets in the predefined sequence of packets are detected.

5. The method of claim 1 wherein the predefined sequence of packets is being selected from packets of the TCP/IP protocol set.

6. The method of claim 5 wherein the TCP/IP protocol set includes a TCP SYN packet, a TCP SYN/ACK packet and TCP RST packet.

7. The method of claim 6 wherein a device at a same source address generates the TCP SYN packet, the TCP RST packet and received the TCP SYN/ACK packet.

8. The method of claim 1 wherein the issuing act further includes the acts of sending a message to an administrator.

9. The method of claim 1 wherein the issuing act further includes the act of blocking future packets from network computers having predefined characteristics.

10. The method of claim 1 wherein the issuing act further includes the act of rate-limiting flows of packets from network devices having predefined characteristics.

11. An intrusion detection system including:

a table containing at least one characteristic identifying network devices and a set of state code corresponding to a sequence in which a predefined set of packets are observed; and

a controller operable to examine received packets, to adjust the state code and to generate an alert if one of the set of state code reaches a predefined value.

12. The intrusion detection system of claim 11 wherein the at least one characteristic includes a Source Address.

13. The intrusion detection system of claim 11 wherein the set of state code corresponding to the sequence of predefined packets includes 00 representing a default, 01 representing a first of the sequence of predefined packets, 10 representing a second of the sequence of predefined packets and 11 representing last of the sequence of predefined packets.

14. The intrusion detection system of claim 11 wherein the predefined set of packets are selected from TCP/IP protocol set.

15. The intrusion detection system of claim 14 wherein selected packets from the TCP/IP protocol set includes SYN, SYN/ACK and RST.

16. The intrusion detection system of claim 11 wherein the controller includes a programmed general purpose computer.

17. The intrusion detection system of claim 11 wherein the controller includes a programmed specialized computer.

18. The intrusion detection system of claim 17 wherein the specialized computer includes a network processor.

19. The intrusion detection system of claim 17 wherein the predefined value includes "11".

20. A program product including:

a medium; and

a computer program recorded on said medium, said computer program including a first set of instructions that examine packets to detect a predefined sequence of packets; and

a second set of instructions that generate an alert if the predefined sequence of packets are detected.

21. The program product of claim 20 further including a third set of instructions responsive to the alert to generate a message notifying an operator of an occurrence of an event.

22. The program product of claim 21 wherein the event indicates unauthorized scanning of a device executing said program product.

23. The program product of claim 20 wherein the predefined sequence of packets are selected from TCP/IP protocol set.

24. The program product of claim 20 wherein the predefined sequence of packets include SYN, SYN/ACK and RST.

25. A method to deploy an intrusion detection system on a network device including acts of:

providing an algorithm to detect a predefined set of packets; and

generating an alert if the predefined set of packets is detected.

26. The method of claim 25 further including the act of providing a table to record at least one characteristic to identify network devices and state code corresponding to a sequence in which the predefined set of packets are received.

27. The method of claim 25 wherein the predefined set of packets is being selected from packets of the TCP/IP protocol set.

28. The method of claim 25 wherein the predefined set of packets includes SYN, SYN/ACK and RST.

29. The method of claim 27 wherein the packets of the TCP/IP protocol set include SYN, SYN/ACK and RST.

30. A method to protect devices from malicious attacks launched on a computer network including the acts of:

providing on a device to be protected a software program that monitors packets; and

issuing an alert if a predefined set of packets are detected.

31. The method of claim 30 wherein the predefined set of packets are detected in a predefined sequence.

32. The method of claim 31 wherein the predefined sequence includes a SYN packet, a SYN/ACK packet and an RST packet provided in the order of recitation.

33. The method of claim 32 wherein a single Source Address (SA) issues the SYN and RST packets and receives the SYN/ACK packet.

34. The method of claim 30 wherein the software program includes a table containing codes whose values represent detection of one of the predefined set of packets.

35. The method of claim 34 wherein the table further includes at least one source Address (SA) associated with at least one of the codes.